POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

TITULO	Política de seguridad y privacidad de la información
Autor	Ing. Jenixe Mena Córdoba
Tema	Políticas generales y específicas de seguridad y privacidad de la información
Fecha de elaboración	Enero de 2024
Formato	PDF
Versión	1.2

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Para la Corporación Autónoma Regional para el Desarrollo Sostenible del Chocó – CODECHOCÓ, la información es un activo fundamental para la prestación de sus servicios, el cumplimiento de sus objetivos misionales y la toma de decisiones eficientes y coherentes frente a su papel como máxima autoridad ambiental del Departamento del Chocó. Por esta razón es necesario velar por la protección y conservación de este importante activo como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

Esta realidad le permite a CODECHOCÓ visualizar la necesidad de implementar un sistema de gestión de seguridad de la información - SGSI como herramienta para identificar y minimizar los riesgos a los cuales están expuestos los activos de información, establecer una cultura de seguridad y garantiza el cumplimiento de los requisitos legales, contractuales, regulatorios y de negocio vigentes.

El proceso de análisis de riesgos de la información y sus activos es el soporte principal para la construcción de esta políticas de seguridad y privacidad, la cual será liderada por la Oficial de Seguridad de la Información, o quien haga sus veces y examinada con regularidad como parte del proceso de revisión por dirección, o cuando se identifiquen cambios en el negocio, su estructura, sus objetivos o alguna condición que afecten la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados.

2. GLOSARIO

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).
- **Activos de Información y recursos:** se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 20116).
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Política:** Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse

como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).
- **Seguridad digital:** Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- **Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

3. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

3.1. GENERAL

Establecer lineamientos que permitan proteger la Información de CODECHOCO y asegurar su integridad, disponibilidad y confidencialidad, a través de una adecuada gestión del riesgo y teniendo en cuenta los requisitos legales, operativos, tecnológicos, de seguridad y de la entidad, vigentes.

3.2. ESPECÍFICOS

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de CODECHOCO.
- Garantizar la continuidad del negocio frente a incidentes.

4. ALCANCE

La Política de Seguridad y Privacidad de la Información de CODECHOCO, aplica para todos sus funcionarios, contratistas, aprendices, practicantes, proveedores, terceros y ciudadanía en general, que tengan acceso a la información de la entidad a través de los documentos, equipos de cómputo, infraestructura tecnológica y canales de comunicación de la Institución.

5. ROLES Y RESPONSABILIDADES

El ***Comité de Seguridad de la Información de la institución***, o quien haga sus veces, es responsable de revisar y proponer para su aprobación, el texto de la Política de Seguridad y Privacidad de la Información, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejora del Sistema de Gestión de Seguridad de la institución. Es responsabilidad de dicho comité definir las estrategias de capacitación en materia de seguridad de la información al interior de la entidad.

Los Propietarios de activos de información son responsables de la identificación, clasificación, mantenimiento y actualización de activos de información; así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener permisos de acceso a la información de acuerdo con sus funciones y competencia. En general, tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

El ***Jefe de Recursos Humanos y el Secretario General***, tendrán la responsabilidad notificar al personal de planta y contratistas, respectivamente, de las obligaciones respecto del cumplimiento de esta política y de sus modificaciones, al

igual que de todos los estándares, procesos, procedimientos, prácticas y guías que surjan del Sistema de Gestión de la Seguridad de la Información. Podrán hacerlo a través de la suscripción de los Compromisos de Confidencialidad o responsabilidades contractuales.

El ***jefe de la Oficina TIC*** debe seguir los lineamientos de la presente política y cumplir los requerimientos que en materia de seguridad informática se establezcan para la operación, administración, comunicación y mantenimiento de los sistemas de información y los recursos de tecnología de la entidad.
Corresponde a dicha jefatura determinar el inventario de activos de información y recursos tecnológicos de los cuales son propietarios o custodios, así como gestionar el inventario institucional de activos de información.

El ***jefe de la Oficina Jurídica*** verificará el cumplimiento de la presente Política en la gestión de todos los contratos, convenios, acuerdos u otra documentación de la entidad con empleados y con terceros. Asimismo, asesorará en materia legal a la entidad en lo que se refiere a la seguridad de la información.

Los ***usuarios*** de la información y de los sistemas utilizados para su procesamiento son responsables de conocer y cumplir la Política de Seguridad y privacidad de la Información vigente.

La ***Oficina de Control Interno*** es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión de activos de información y la tecnología de información. Es su responsabilidad informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

6. NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

7. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

7.1. POLÍTICA CORPORATIVA

La Dirección General de la Corporación Autónoma Regional para el Desarrollo Sostenible del Chocó – CODECHOCÓ, entendiendo la importancia de una adecuada gestión de la información, se compromete con la implementación de un sistema de gestión de seguridad de la información – SGSI, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para CODECHOCÓ, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

7.2. POLÍTICAS GENERALES

CODECHOCO ha establecido las siguientes Políticas Generales de Seguridad de la Información, las cuales representan la visión de la Institución en cuanto a la protección de sus activos de Información:

1. Existirá un Comité de Seguridad de la Información, que será el responsable del mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información SGSI.

2. Los activos de información de CODECHOCO, serán identificados y clasificados para establecer los mecanismos de protección necesarios.

3. CODECHOCO definirá e implantará controles para proteger la información contra violaciones de autenticidad, accesos no autorizados (electrónicos o físicos), la perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la Entidad.

4. Todos los funcionarios, contratistas, practicantes, aprendices y terceros serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

5. Se realizarán auditorías y controles periódicos sobre el modelo de gestión de Seguridad de la Información de CODECHOCO.

6. Únicamente se permitirá el uso de software autorizado que haya sido adquirido legalmente por la Institución.

7. Es responsabilidad de todos los funcionarios y contratistas de CODECHOCO reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que identifiquen.

8. Las violaciones a las Políticas y Controles de Seguridad de la Información serán reportadas, registradas y monitoreadas.

9. CODECHOCÓ protegerá la información generada, procesada o resguardada por sus procesos, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros.

10. CODECHOCÓ garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

11. CODECHOCÓ implementará control de acceso a la información, sistemas y recursos de red.
12. CODECHOCÓ garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

13. CODECHOCÓ contará con un Plan de Continuidad del Negocio que asegure la continuidad de las operaciones, ante la ocurrencia de eventos no previstos o desastres naturales.

7.3. POLÍTICAS ESPECIFICAS

Adicionalmente CODECHOCO cuenta con políticas específicas y un conjunto de estándares y procedimientos que soportan la política corporativa.

Acuerdos de confidencialidad [ISO/IEC 27001:2005 A.6.1.5]

Todos los funcionarios de CODECHOCO y/o terceros deben aceptar los acuerdos de confidencialidad definidos por la Institución, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella. Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de CODECHOCO a personas o entidades externas. Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

Riesgos relacionados con terceros [ISO/IEC 27001:2005 A.6.2.2]

CODECHOCO identifica los posibles riesgos que pueden generar el acceso, procesamiento, comunicación o gestión de la información y la infraestructura para su procesamiento por parte de los terceros, con el fin de establecer los mecanismos de control necesarios para que la seguridad se mantenga. Los controles que se establezcan como necesarios a partir del análisis de riesgos, deben ser comunicados y aceptados por el tercero mediante la firma de acuerdos, previamente a la entrega de los accesos requeridos.

Uso adecuado de los activos [ISO/IEC 27001:2005 A.7.1.3] [Acuerdos 047 y 056 de 2000 Archivo General de la Nación]

El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos públicos, a la competencia del área o dependencia específica y a los permisos y niveles de acceso de los funcionarios y contratistas determinadas por los jefes de área o dependencia. Para la consulta de documentos cargados en el software de gestión documental, o el que haga sus veces, se establecerán privilegios de acceso a los funcionarios y/o contratistas de acuerdo con el

desarrollo de sus funciones y competencias. Dichos privilegios serán establecidos por el jefe o director del área, quien comunicará al grupo encargado de la administración del software el listado con los funcionarios y sus privilegios.

Todos los funcionarios y terceros que manipulen información en el desarrollo de sus funciones deberán firmar un "acuerdo de confidencialidad de la información", donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información; y que cualquier violación a lo establecido en este parágrafo será considerada como un "incidente de seguridad".

Acceso a Internet

El internet es una herramienta de trabajo que permite navegar en muchos otros sitios relacionados o no con las actividades propias de CODECHOCO, por lo cual el uso adecuado de este recurso se debe controlar, verificar y monitorear, considerando, para todos los casos, los siguientes lineamientos:

a) No está permitido:

- El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.

- El acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, páginas de streming, redes sociales, Net2phone y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio de CODECHOCO.

- El intercambio no autorizado de información de propiedad de CODECHOCO, de sus clientes y/o de sus funcionarios, con terceros.

- La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.

- La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el jefe respectivo y la oficina Sistemas, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

b) CODECHOCO debe realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los funcionarios y/o terceros. Así mismo, puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo a la legislación nacional vigente.

c) Cada uno de los usuarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

d) Los funcionarios y terceros, al igual que los empleados o subcontratistas de estos, no pueden asumir en nombre de CODECHOCO, posiciones personales en encuestas de opinión, foros u otros medios similares.

e) El uso de Internet no considerado dentro de las restricciones anteriores, es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de CODECHOCO.

Correo electrónico

Los funcionarios y terceros autorizados a quienes CODECHOCO les asigne una cuenta de correo deberán seguir los siguientes lineamientos:

a) La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro de CODECHOCO, así mismo podrá ser utilizada para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad.

b) Los mensajes y la información contenida en los buzones de correo son propiedad de CODECHOCÓ, y cada usuario como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

c) El tamaño de los buzones de correo es determinado por la oficina de TI de acuerdo con las necesidades de cada usuario y previa autorización del jefe de la dependencia correspondiente.

d) El tamaño de envío y recepción de mensajes, sus contenidos y demás características propias de estos deberán ser definidos e implementados por oficina de sistemas.

e) No es permitido:

- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Institución, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra

de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.

- Utilizar la dirección de correo electrónico institucional como punto de contacto en comunidades interactivas de contacto social, tales como facebook y/o myspace, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales.

- El envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

- El envío de archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por la dirección respectiva y la oficina de TI.

f) El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo institucional proporcionada.

g) El envío masivo de mensajes publicitarios corporativos deberá contar con la aprobación de la oficina de comunicaciones y la autorización de la oficina de TI. Además, para terceros se deberá incluir un mensaje que le indique al destinatario como ser eliminado de la lista de distribución. Si una dependencia debe, por alguna circunstancia, realizar envío de correo masivo, de manera frecuente, este debe ser enviado a través de una cuenta de correo electrónico a nombre de la dependencia respectiva y/o servicio habilitado para tal fin y no a través de cuentas de correo electrónico asignadas a un usuario particular.

h) Toda información de CODECHOCO generada con los diferentes programas computacionales (Ej. Office, Project, Access, Wordpad, etc.), que requiera ser enviada fuera de la Entidad, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables, utilizando las características de

seguridad que brindan las herramientas proporcionadas por la oficina de sistemas. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

i) Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por CODECHOCO, a través de la oficina de comunicaciones, y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

Recursos tecnológicos

El uso adecuado de los recursos tecnológicos asignados por CODECHOCO a sus funcionarios y/o terceros se reglamenta bajo los siguientes lineamientos:

a) La instalación de cualquier tipo de software o hardware en los equipos de cómputo de CODECHOCO es responsabilidad de la oficina de TI, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por e CODECHOCO a través de esta Dirección.

b) Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo, entre otros. Estos cambios pueden ser realizados únicamente por el personal de la oficina de TI.

c) La oficina de TI debe definir y actualizar, de manera periódica, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

d) Únicamente los funcionarios y terceros autorizados por la oficina de TI, previa solicitud gestionada a través de la mesa de servicios por parte de la dependencia que lo requiera, pueden conectarse a la red inalámbrica de CODECHOCO.

e) La conexión a redes inalámbricas externas para usuarios con equipos portátiles que estén fuera de la oficina y que requieran establecer una conexión a la infraestructura tecnológica de CODECHOCO, debe hacerse bajo los esquemas y herramientas de seguridad autorizados y establecidos por la oficina de TI.

f) Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de CODECHOCO; las conexiones establecidas para este fin, deben utilizar los esquemas y herramientas de seguridad y administración definidos por la oficina de TI.

g) La sincronización de dispositivos móviles, tales como PDAs, smartphones, celulares u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la organización, debe estar autorizado de forma explícita por la dependencia respectiva, en conjunto con la oficina de TI y podrá llevarse a cabo sólo en dispositivos provistos por la organización, para tal fin.

Control de acceso físico [ISO/IEC 27001:2005 A.9.1]

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales. De igual forma, los centros de cómputo, cableado y cuartos técnicos de las

oficinas deben contar con mecanismos que permitan garantizar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.), especificados por los fabricantes de los equipos que albergan y que pueden responder de manera adecuada ante incidentes como incendios e inundaciones.

Protección y ubicación de los equipos [ISO/IEC 27001:2005 A.11.1]

Los equipos que hacen parte de la infraestructura tecnológica de CODECHOCO tales como, servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aires acondicionados, plantas telefónicas, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan y/o brinden servicios de soporte a la información crítica de las dependencias, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos. De igual manera, se debe adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

Los funcionarios y terceros, incluyendo sus empleados o subcontratistas, que tengan acceso a los equipos que componen la infraestructura tecnológica de CODECHOCO no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos. CODECHOCO mediante mecanismos adecuados monitoreará las condiciones ambientales de las zonas donde se encuentren los equipos (Centros de Cómputo).

Segregación de funciones [ISO/IEC 27001:2005 A.9.1]

Toda tarea en la cual los funcionarios tengan acceso a la infraestructura tecnológica y a los sistemas de información, debe contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y los privilegios correspondientes, con el

fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de la organización. En concordancia:

- Todos los sistemas de disponibilidad crítica o media de la entidad, deben implementar las reglas de acceso de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

- Los módulos ejecutables nunca deberán ser trasladados directamente de las librerías de pruebas a las librerías de producción sin que previamente sean compilados por el área asignada para tal efecto, que en ningún momento deberá ser el área de desarrollo ni la de producción.

- El nivel de súper usuario de los sistemas debe tener un control dual, de tal forma que exista una supervisión a las actividades realizadas por el administrador del sistema.

- Deben estar claramente segregadas las funciones de soporte técnico, planificadores y operadores.

Protección contra software malicioso [ISO/IEC 27001:2005 A.12.2]

CODECHOCO establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, firewall, antispam, antispyware y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso del mismo a la red institucional, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código móvil y malicioso. Será responsabilidad de la oficina de TI autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados bajo ninguna

circunstancia, así como de su actualización permanente. Así mismo, CODECHOCO define los siguientes lineamientos:

a) No está permitido:

- La desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por CODECHOCO.

- Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.

- Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.

- El uso de código móvil. Éste sólo podrá ser utilizado si opera de acuerdo con las políticas y normas de seguridad definidas y debidamente autorizado por la oficina de TI.

Copias de respaldo [ISO/IEC 27001:2005 A.12.3.1]

CODECHOCO debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por la Oficina de TI y las dependencias responsables de la misma, contenida en la plataforma tecnológica de la Institución, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad.

Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado. La oficina de TI establecerá

procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y definirá conjuntamente con las dependencias los períodos de retención de la misma. Adicionalmente, debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada. Los medios magnéticos que contienen la información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguardan dichas copias, debe tener los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiados.

Gestión de medios removibles [ISO/IEC 27001:2005 A.8.3.1

El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, USBs, memorias flash, discos duros externos, Ipods, celulares, cintas) sobre la infraestructura para el procesamiento de la información de CODECHOCO, estará autorizado para aquellos funcionarios cuyo perfil del cargo y funciones lo requiera. La Oficina de TI es responsable de implementar los controles necesarios para asegurar que en los sistemas de información de CODECHOCO sólo los funcionarios autorizados pueden hacer uso de los medios de almacenamiento removibles. Así mismo, el funcionario se compromete a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información de CODECHOCO que éste contiene.

Intercambio de información [ISO/IEC 27001:2005 A.13.2]

CODECHOCO firmará acuerdos de confidencialidad con los funcionarios, clientes y terceros que por diferentes razones requieran conocer o intercambiar información restringida o confidencial de la Institución. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se

deberán firmar antes de permitir el acceso o uso de dicha información. Todo funcionario de CODECHOCÓ es responsable de proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada. Los propietarios de la información que se requiere intercambiar son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad y requeridos.

Control de acceso lógico [ISO/IEC 27001:2005 A.9.1]

El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información de CODECHOCO debe ser asignado de acuerdo a la identificación previa de requerimientos de seguridad y del negocio que se definan por las diferentes dependencias de la Institución, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información. Los responsables de la administración de la infraestructura tecnológica de CODECHOCÓ asignan los accesos a plataformas, usuarios y segmentos de red de acuerdo a procesos formales de autorización. La autorización para el acceso a los sistemas de información debe ser definida y aprobada por la dependencia propietaria de la información, o quien ésta defina, y se debe otorgar de acuerdo con el nivel de clasificación de la información identificada, según la cual se deben determinar los controles y privilegios de acceso que se pueden otorgar a los funcionarios y terceros e implementada por la oficina de sistemas. Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de procesamiento de información de CODECHOCO, sea por Internet, acceso telefónico o por otro medio, siempre debe estar autenticado y sus conexiones deberán utilizar cifrado de datos.

Gestión de contraseñas de usuario [ISO/IEC 27001:2005 A.9.4.3]

Todos los recursos de información críticos del CODECHOCO tienen asignados los privilegios de acceso de usuarios con base en los roles y perfiles que cada funcionario requiera para el desarrollo de sus funciones, definidos y aprobados por las áreas de negocio y administrados por la oficina de sistemas. Todo funcionario o tercero que requiera tener acceso a los sistemas de información de CODECHOO debe estar debidamente autorizado y debe acceder a dichos sistemas haciendo uso, como mínimo, de un usuario (ID) y contraseña (password) asignados por la organización. El funcionario debe ser responsable por el buen uso de las credenciales de acceso asignadas.

Escritorio y pantalla limpia [ISO/IEC 27001:2005 A.9.4.1]

Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los funcionarios de CODECHOCÓ deben mantener la información restringida o confidencial bajo llave cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye: documentos impresos, CDs, dispositivos de almacenamiento USB y medios removibles en general. Adicionalmente, se requiere que la información sensible que se envía a las impresoras sea recogida manera inmediata. Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados. Todas las estaciones de trabajo deberán usar el papel tapiz y el protector de pantalla corporativo, el cual se activará automáticamente después de cinco (5) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

Identificación de requerimientos de seguridad [ISO/IEC 27001:2005 A.14.2.1]

La inclusión de un nuevo producto de hardware, software, aplicativo, desarrollo interno o externo, los cambios y/o actualizaciones a los sistemas existentes en CODECHOCO, deben

estar acompañados de la identificación, análisis, documentación y aprobación de los requerimientos de seguridad de la información, labor que debe ser responsabilidad de la oficina de sistemas y las dependencias propietarias del sistema en cuestión. Los requerimientos de seguridad de la información identificados, obligaciones derivadas de las leyes de propiedad intelectual y derechos de autor deben ser establecidos en los acuerdos contractuales que se realicen entre CODECHOCO y cualquier proveedor de productos y/o servicios asociados a la infraestructura de procesamiento de información. Es responsabilidad de la oficina de TI garantizar la definición y cumplimiento de los requerimientos de seguridad de la Información y en conjunto con la secretaria general establecer estos aspectos con las obligaciones contractuales específicas.

Control de Cambios

Fecha	Autor	Versión	Cambio
Junio de 2018	Jenixe Mena	1.0	Creación del documento
Enero de 2020	Jenixe Mena	1.1	Correcciones de forma, actualización de controles
Enero de 2024	Jenixe Mena	1.2	Adición de roles y responsabilidades, definición de nuevas políticas